UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,267	03/25/2004	Jan Camenisch	CH920020054US1	6902

48233 7590 06/11/2008
SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 GARDEN CITY PLAZA
SUITE 300
GARDEN CITY, NY 11530

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/809,267	**Applicant(s)** CAMENISCH ET AL.	
	Examiner FATOUMATA TRAORE	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-14,16 and 18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12-14, 16 and 18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on arch 27, 2008 has been entered.

Claims Status

Claims 1, 5, 7, 9, 10 , 12, 14, 16 and 18 have been amended; Claims 11, 15 17 and 19-21 have been cancelled; Claims 1-10, 12-14, 16 and 18 are pending and have been considered below.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

3. Claims 5, 9 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. the claims recite the limitation of : "*with a probability close to certainty*". It is unclear to the examiner what applicant is trying to claim. For examination purpose only, the examiner will interpret the claims as follow: "*selecting an exponent value from an exponent interval I having a plurality of exponent*

elements, said interval having a specified first random limit, wherein each element of said plurality of exponent elements of the exponent interval I has a unique prime factor that is larger than a given security parameter". Appropriate correction is required.

4. Claims 1, 7, 10, 12, 14 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. the claims recite the limitation of : "*providing a public key comprising an exponent-interval description including said first random limit, and an interval width specification and a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret key, said exponent interval, and two public values from a set of elements having a square root modulo n, such that the random secret key and a selected exponent value from the plurality of exponent elements in said exponent interval ! are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification*" it is unclear to the examiner how the signature is generated, to where the public is provided and how the verification is performed. It is also unclear to the examiner what applicant is try to say by "*with a probability close to certainty*". Appropriate correction is required.

5. Claim 1 recites the limitation "said interval" in line 5. There is insufficient antecedent basis for this limitation in the claim.

6. Claim 1 recites the limitation "said secret key" in line 12. There is insufficient antecedent basis for this limitation in the claim.

applicant is required to check and correct antecedent basis problem for similar claims 7, 10, 12, 14 and 18.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 9, 10 and 12 are drawn to a computer program per se. The claims recite the limitation of "means for selecting, means for providing, means for deriving, etc". However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer programs modules(see specification page 14). A computer program is not a series of steps or acts and this is not a process. A computer program is not a physical article or object and as such is not a machine or manufacture. A computer program is not a combination of substances and therefore not a compilation of matter. Thus, a computer program by itself does not fall within any of the four categories of invention. Therefore, Claims 9, 10 and 12 are not statutory.

Allowable Subject Matter

9. Claims 1, 7, 10, 12, 14 and 18 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph and the 101 rejection set forth in this Office action.

10. Claims 2-4 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Examiner's Statement of Reasons for Allowance

11. Prior art references were found which disclosed a cryptographic key generation and safekeeping process whereby source code is loaded on a secure computer system with a "master-key" and "locldng-key" compiled from the source code and then stored on disks (Abstract, Col. 12, lines 43-46). Moreover, a public exponent e" which is derived from an RSA modulus N and private exponent d. (Col. 9, lines 19-28) Brennan et al (US 5,675,649), and Arditti et al (US 6,125445) which spoke to determining some sort of interval based on a parameter "m" from which an exponent value "a" that a "claimant" entity can use and an exponent "[3" that a separate "verifier' entity can use when applying hash functions according a special type of technique (called Diffie Helhnan algorithm), this algorithm actually involves the generation of key values by both participants (a "claimant" as shown implementing steps Aa- Ad, Ca-Ce and "verifier" as shown implementing steps Ba-Bfin the paragraph bridging columns 4 and 5)

12. The prior art references of record do not teach or render obvious the limitations as recited in independent claims 1, 7, 10, 12, 14 and 18 specific to providing a public key comprising an exponent-interval description including said first random limit, and an interval width specification and a public key value derived from the random secret key, said public key value including a random prime value, a number (n) corresponding to a product of two large prime numbers forming said secret keg, said exponent interval, and

two public values from a set of elements having a square root modulo n, such that the random secret key and a selected exponent value from the plurality of exponent elements in said exponent interval ! are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.

Response to Arguments

13. Applicant's arguments with respect to claims 5-6, 9 and 16 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 5, 9 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Brennan et al** (US 5675649) in view of ***Lambert et al*** (US 7,127,063).

Claims 5, 9 and 16: **Brennan et al** discloses a method for cryptographic key generation comprising the steps of:

selecting an exponent value from an exponent interval I having a plurality of exponent elements, said interval having a specified first random limit, wherein each element of said plurality of exponent elements of the exponent interval I has, with a probability, close to certainty, a unique prime factor that is larger than a given security parameter (M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary expansion as does N. Absent specific knowledge of p or q. M must be presumed computationally infeasible to factor) (column 10, lines 47-51); and deriving the signature value from a provided secret key, the selected exponent value from said plurality of exponent elements in said exponent interval I, and the message, the signature value being sendable within the network to a second computer node for verification (a third stage comprises creation of a self –signed certificate attesting the certificate authority name, public module N, and public exponent e and the validity period of these public key parameters. A secure hash function is applied to the certificate information to create a message digest, ext the message digest is encrypted with the certificate authority's secret key)(column 12, lines 22-30).

However, does not explicitly disclose that the value of the exponent lies in a specific interval. However, **Lambert et al** discloses a method, apparatus and computer storage medium, which further discloses a method of publicly verifiable encryption by proving that the committed number belongs to an interval) (column 4, lines 25-35). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to set an interval value for the exponent in **Brennan et al**' disclosure. One would have been motivated to do so in order to ensure integrity and authenticity of data and often also confidentiality.

16. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Brennan et al** (US 5675649) in view of **Lambert et al** (US 7,127,063) as applied to claim 5 above, and in further view of **Matyas et al** (US 5265164).

Claim 6: **Brennan et al** and **Lambert et al** disclose a method for cryptographic key generation as in claim 5 above, but does not explicitly disclose that the step of deriving the signature value further comprises a computation of the i-th root of a value derived from the message and the secret key using a cryptographic hash function, the i being the exponent value. However, **Matyas et al** discloses a method for providing a secure hash and sign signature, which further discloses the step of deriving the signature value further comprises a computation of the i-th root of a value derived from the message and the secret key using a cryptographic hash function (at step 224, the encrypted CFBDKB (i.e., ECFBDKB) is decrypted with the public key algorithm using PRAb, the private device authentication key of device B. PRAb is stored in the CF Environment 146' of the CF 30', and hence is available for use by the ICFER instruction. For example, if the public key algorithm is the RSA algorithm, then decryption consists of raising the ECFBDKB to the power of an exponent d modulo a modulus n, where d and n constitute the private key) (column 37, lines 14-23). Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to modify the combined teaching of **Brennan et al** and **Lambert et al** such as to add a step of generating the signature by computing the i-th root. One would have been motivated to do so in order to ensure integrity and authenticity of data and often also confidentiality.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Friday, June 6, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136